WILLKIE FARR & GALLAGHER LLP
BENEDICT Y. HUR (SBN: 224018)
bhur@willkie.com
SIMONA AGNOLUCCI (SBN: 246943)
sagnolucci@willkie.com
EDUARDO E. SANTACANA (SBN: 281668)
esantacana@willkie.com
ARGEMIRA FLÓREZ (SBN: 331153)
aflorez@willkie.com
HARRIS MATEEN (SBN: 335593)
hmateen@willkie.com
333 Bush Street, 34th Floor
San Francisco, CA 94104
Telephone: (415) 858-7400

Attorneys for Defendant
GOOGLE LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

ANIBAL RODRIGUEZ, et al. individually and on behalf of all others similarly situated,

Plaintiff,

vs.

GOOGLE LLC,

Defendant.

Case No. 3:20-CV-04688-RS

GOOGLE LLC'S STATEMENT IN SUPPORT OF OMNIBUS MOTION TO SEAL PORTIONS OF [DKT. NOS. 470, 478, 485]

(CIVIL LOCAL RULE 79-5)

Date:	May 15, 20225
Time:	1:30 p.m.
Ctrm:	3 - 17th Floor
Judge:	Hon. Richard Seeborg
Action Filed:	July 14, 2020
Trial Date:	August 18, 2025

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

I. INTRODUCTION

Pursuant to Civil Local Rule 79-5 and the Court's April 23, 2025 Order for an omnibus motion to seal (Dkt. 484), Defendant Google LLC ("Google") submits this statement setting forth the compelling reasons supporting its requests to seal portions of the briefing and exhibits filed in connection with the following recent evidentiary motions: Plaintiffs' Motion to Exclude Certain Opinions and Testimony of Google's Experts ("*Daubert* Motion") (Dkt. 473), Google's Opposition thereto (Dkt. 488), Plaintiffs' Opposition to Google's Motion to Exclude Sundar Pichai from Testifying at Trial ("Pichai Opp.") (Dkt. 479), and Google's Reply thereto ("Google's Pichai Reply") (Dkt. 487). Google also seeks, pursuant to Civil Local Rule 79-5(b), to maintain under seal certain previously sealed information referenced in these filings. Declaration of David Monsees ("Monsees Decl.") ¶ 3.[1]

As these evidentiary motions address the admissibility of expert opinions and trial testimony, its contents are considered to be "more than tangentially related to the merits of [the] case." *Ctr. for Auto Safety v. Chrysler Grp., LLC*, 809 F.3d 1092, 1099 (9th Cir. 2016). Therefore, the Ninth Circuit's "compelling reasons" standard governs these sealing requests. *Id.* at 1101. This standard requires a showing of specific reasons for sealing that outweigh the public's interest in access. *Id.*; *Kamakana v. Cty. & Cnty. of Honolulu*, 447 F.3d 1172, 1179 (9th Cir. 2006); *see also, e.g.*, *VLSI Tech. LLC v. Intel Corp.*, 2023 WL 6812546, at *2 (N.D. Cal. Oct. 16, 2023) (applying compelling reasons to *Daubert* materials).

Google seeks to protect specific, limited information falling into categories routinely deemed sealable upon a showing of compelling reasons: (1) competitively sensitive internal consumer studies, metrics, and projections; (2) product design, performance, and improvement deliberations; (3) non-public technical details concerning internal systems; (4) internal codenames and names of technical infrastructure; (5) private employee information. *See Nixon v. Warner Commc'ns, Inc.*, 435 U.S. 589, 598 (1978) (protecting business information); *Apple Inc. v. Psystar*

[1] Pursuant to Civil Local Rule 79-5, a party need not file a motion to seal when a federal statute or prior court order in the same case expressly authorizes the party to file certain documents or portions of documents under seal. Accordingly, Google will not refile them here.

Corp., 658 F.3d 1150, 1161-62 (9th Cir. 2011) (same). As detailed in the accompanying Monsees Declaration (¶¶ 5-28), public disclosure of this information would risk significant competitive injury to Google, create potential security vulnerabilities, and improperly infringe on legitimate employee privacy interests.

Google's requests are narrowly tailored, seeking redaction wherever feasible and requesting to seal entire documents only where sensitive information is pervasive and inextricably intertwined with non-sensitive content, thus making redaction impracticable. Monsees Decl. ¶ 4.Of the 44 exhibits Plaintiffs attached to their Pichai Opposition, Google seeks full sealing for only 9 exhibits where confidential information is pervasive, and requests only minimal, discrete redactions for 22 others. Furthermore, while the compelling reasons standard applies to these filings, the specific public interest in accessing certain discrete portions of information is diminished where, as detailed below and in the Monsees Declaration, the data concerns products or time periods far removed from the core issues remaining in this litigation, or where Plaintiffs' reliance on the underlying document is minimal or does not touch upon the sensitive information Google seeks to protect. This context further supports the conclusion that Google's compelling interests outweigh the public interest for the specific, limited information identified.

Accordingly, Google respectfully requests that the Court grant its limited sealing requests as detailed herein and in the accompanying [Proposed] Order.

II. LEGAL STANDARD

Courts recognize a general right to inspect and copy public records, including judicial records. *Kamakana*, 447 F.3d at 1178 (quoting *Nixon*, 435 U.S. at 597). This right, however, is not absolute. *Id*. To overcome the presumption of access for documents "more than tangentially related to the merits of a case," the party seeking sealing must demonstrate "compelling reasons" supported by specific factual findings that outweigh the public's interest in disclosure. *Ctr. for Auto Safety*, 809 F.3d at 1097-99. Courts generally apply the "compelling reasons" standard to motions related to the admissibility of evidence at trial. *See id.* at 1099; *see also, e.g., Skillz Platform Inc. v. AviaGames Inc.*, 2023 WL 8817418, at *1 (N.D. Cal. Dec. 20, 2023); *VLSI*, 2023 WL 6812546, at *1; *Palantir Technologies Inc. v. Abramowitz*, 2022 WL 2674200, at *2 (N.D.Cal., 2022).

"Compelling reasons" typically exist when sealing is necessary to protect trade secrets or prevent the use of "sources of business information that might harm a litigant's competitive standing." *Nixon*, 435 U.S. at 598; see also *Psystar*, 658 F.3d at 1161-62 (protecting confidential business plans and technical information); *In re Elec. Arts, Inc.*, 298 F. App'x 568, 569 (9th Cir. 2008). This includes sensitive financial data, marketing strategies, product development plans, internal analyses, and technical operational details. *See, e.g., Apple Inc. v. Samsung Elecs. Co.*, 727 F.3d 1214, 1228 (Fed. Cir. 2013) (internal market research); *Adtrader, Inc. v. Google LLC*, 2020 WL 6391210, at *1 (N.D. Cal. Mar. 24, 2020) (marketing strategies, product plans); *Finjan, Inc. v. Proofpoint, Inc.*, 2016 WL 7911651, at *2 (N.D. Cal. Apr. 6, 2016) (technical information). Compelling reasons may also exist to protect against security vulnerabilities or safeguard legitimate privacy interests, such as non-public employee information or confidential personnel records. *See, e.g., In re Google Inc. Gmail Litig.*, 2013 WL 5366963, at *3 (N.D. Cal. Sept. 25, 2013) (security risks); *E. & J. Gallo Winery v. Instituut Voor Landbouw-En Visserijonderzoek*, 2018 WL 4961606, at *2 (E.D. Cal. Oct. 12, 2018) (employee privacy). Generalized claims of harm or embarrassment are insufficient. *See Kamakana*, 447 F.3d at 1178-79.

The sealing request must also be "narrowly tailored" to seal only the specific information requiring protection. Civ. L. R. 79-5(c)(3); *Press-Enter. Co. v. Superior Court*, 464 U.S. 501, 510 (1984). Parties must use the least restrictive means, such as redaction, whenever possible. Civ. L. R. 79-5(c)(3).

III. DISCUSSION

Google's limited sealing requests fall into categories previously recognized by courts as protectable under the compelling reasons standard. Each request is narrowly tailored to protect specific sensitive information, based on particularized showings of potential harm set forth in the accompanying Monsees Declaration. Furthermore, as detailed below, much of the information sought for sealing is only tangentially related to the merits of Plaintiffs' motion regarding Mr. Pichai, concerning different products, features, or time periods, or Plaintiffs rely on the documents in question for general propositions where the specific sensitive details Google seeks to protect are unnecessary for the public's understanding of the dispute.

A. Commercially Sensitive Proprietary Business and Technical Information

Compelling reasons exist to seal "sources of business information that might harm a litigant's competitive standing." *In re Electronic Arts*, 298 F. App'x at 569 (quoting *Nixon*, 435 U.S. at 598); *Psystar*, 658 F.3d at 1162 (preventing competitors from gaining "unfair insight"). Public disclosure of the information discussed below—reflecting Google's internal strategies, proprietary research, confidential performance metrics, sensitive customer data, and product development deliberations—would provide competitors an unearned windfall, potentially undermining Google's significant investments and market position. *See Ojmar US, LLC v. Sec. People, Inc.*, 2016 WL 6091543, at *2 (N.D. Cal. Oct. 19, 2016).

1. Competitively Sensitive Internal Consumer Studies, Metrics, and Projections

A litigant's competitive standing can be harmed through the disclosure of internal market research, performance metrics, and strategy, as competitors can use this information against them. *See Apple v. Samsung*, 727 F.3d at 1228; *Algarin v. Maybelline, LLC*, 2014 WL 690410, at *3 (S.D. Cal. Feb. 21, 2014) (sealing consumer research, sales data, and product plans to prevent competitors from replicating practices without investment). The following documents reflect Google's internal analysis, customer studies, performance metrics, and projections, which it has expended significant resources to conduct and maintain as confidential:

- In **Exhibit 11**[2], an internal presentation overviewing Google Analytics for Firebase, Google seeks to seal specific slides (pages -885 through -915) containing early-stage internal brainstorming, described as "design concepts" and "what-if" scenarios for potential future product development. Monsees Decl. ¶ 11.
- In **Exhibit 12**, an internal presentation discussing user engagement with Firebase, Google seeks narrow redactions covering pages -763 through -766. These pages contain confidential case studies that identify specific third-party customers by name and provide details about the concrete performance data and results these customers achieved using Google's services, information sensitive to both Google and its customers. Monsees Decl. ¶ 12.

[2] All Exhibits referenced are Exhibits to Plaintiffs' Opposition to Google's Motion to Exclude Sundar Pichai from Testifying at Trial (Dkt. 479), unless otherwise specified.

- In **Exhibit 32**, an internal Google email chain, Google proposes a very narrow redaction on page -845. This redaction protects a specific, non-public internal statistic that quantifies user interaction metrics related to the usage of certain account-level control toggles. Monsees Decl. ¶ 18.
- In **Exhibit 34**, an internal Google email thread providing updates for Google's marketing leadership, Google seeks limited redactions on page -484. These redactions shield confidential internal statistics measuring user activity, specifically Daily Active Users (DAUs), and detailed traffic data observed on various platforms following a Super Bowl advertising campaign. Monsees Decl. ¶ 20.

The information Google seeks to protect in these exhibits constitutes classic examples of competitively sensitive business data. Exhibit 11 reveals forward-looking strategic thinking and potential product evolution insights that competitors could exploit. Monsees Decl. ¶ 11. Exhibit 12 contains confidential customer data—naming specific clients and their performance results—the disclosure of which could harm Google's customer relationships and allow competitors to target those customers or benchmark against Google's service effectiveness using non-public data. Monsees Decl. ¶ 12. Exhibits 32 and 34 contain specific, non-public internal performance metrics about user engagement and marketing campaign effectiveness, valuable intelligence for competitors seeking to gauge Google's success or refine their own strategies. Monsees Decl. ¶¶ 18, 20. Disclosure of this category of information—internal strategic concepts, confidential customer performance data, and specific internal metrics—would cause competitive harm by providing rivals with unearned insights into Google's strategies, performance, and customer successes. *See Apple v. Samsung*, 727 F.3d at 1228; *Algarin*, 2014 WL 690410, at *3. Google's requests are narrowly tailored, seeking to seal only specific forward-looking slides (Ex. 11) or redact discrete customer case studies and internal data points (Ex. 12, 32, 34), leaving the remaining content accessible. Plaintiffs' Opposition cites different portions of these exhibits, and Google's requests would not affect Plaintiffs' ability to make their arguments or the public's understanding of the underlying dispute.

2. Product design, performance, and improvement deliberations and presentations

Courts routinely find compelling reasons to seal documents containing forward-looking strategy, internal assessments, and deliberations that inform product design, reflect performance, or

guide improvements, as disclosure can reveal roadmaps and weaknesses to competitors. *See Adtrader*, 2020 WL 6391210, at *1; *Network Appliance, Inc. v. Sun Microsystems, Inc.*, 2010 WL 841274, at *2 (N.D. Cal. Mar. 10, 2010). Google seeks to seal or redact such competitively sensitive information in the following exhibits:

- Google seeks to seal **Exhibit 2**, a document containing internal engineering–product management meeting notes, in its entirety. These notes discuss ongoing strategy, technical challenges encountered (like data scaling and latency), progress updates on feature rollouts, and specific details about Google's internal systems—such as data storage architecture, server configurations, and internal code libraries—related to user account controls. Sensitive commercial and technical information is pervasive throughout the document. Monsees Decl. ¶ 6.

- Google seeks to seal **Exhibit 4** in its entirety. an internal Product Requirements Document (PRD), a type of foundational strategic document at Google. It outlines confidential proposals for new or updated features, reflecting internal analyses, strategic planning, specific metrics targets, product goals, technical approaches, and proprietary research resulting from significant investment. Monsees Decl. ¶ 7.

- In **Exhibit 8**, an internal presentation concerning Google's Firebase platform, Google seeks only to redact a specific chart found on the page ending -951. This chart displays sensitive internal analysis regarding the business impact and competitive positioning of Firebase services relative to named rivals. Monsees Decl. ¶ 8.

- In **Exhibit 9**, an internal document detailing Firebase's history, Google seeks only to redact specific Objectives and Key Results (OKRs) appearing on pages ending -981 and -982. These OKRs reveal confidential internal strategic priorities, quantifiable goals (like growth rates or launch timelines), and internal performance targets for the Firebase organization. Monsees Decl. ¶ 9.

- Google seeks to seal **Exhibit 10** in its entirety. This document is an employee's "perf packet," prepared for a performance review cycle. It compiles confidential, proprietary technical details about product functions and data systems, specific statistics and customer information related to the employee's projects within the Firebase portfolio, and is interwoven with highly sensitive personal employee performance information (self-assessment, reviews, goals). Monsees Decl. ¶ 10.

- Google seeks to seal **Exhibit 19** in its entirety. This document contains extensive internal notes from leadership meetings within Google's Geo organization (responsible for Maps, Earth, and other location-related products), spanning approximately eight months in 2018. These notes detail product roadmaps, launch timelines, confidential key performance indicators (KPIs), internal goals (DAUs, revenue targets, NPS data), internal performance critiques, competitive intelligence, and market analysis across multiple Geo products, much of which is unrelated to this case. Monsees Decl. ¶ 13.

- In **Exhibit 20**, an email summarizing an internal "Google Leads" meeting, Google seeks narrow redactions on pages ending -151 and -152. These redactions cover sensitive internal discussions about managing potential leaks, confidential commercial information including negotiation strategies with partners/competitors, and internal competitive assessments—all unrelated to the specific points Plaintiffs cite from this document. Monsees Decl. ¶ 14.

- In **Exhibit 29**, an internal strategy document addressing changes to default retention settings for WAA, YouTube History, and Location History, Google seeks specific redactions on page -126, and on pages-136 through -143. These cover sensitive technical implementation details (including pipelines, downstream systems, identifiers, bug tracking), discussions involving legal review, and insights derived from confidential user research studies. Monsees Decl. ¶ 17.

- Google seeks to seal **Exhibit 33** in its entirety. This is an internal document prepared by Google's Privacy and Data Protection Office following a significant internal fact-gathering project. Marked with access restrictions, it compiles information from confidential interviews with numerous employees across various products (like Docs, Gmail, Maps) regarding potential feature changes and privacy considerations. This research directly informs Google's confidential product roadmap and strategic decisions. It represents a comprehensive compilation of resource-intensive internal research and could offer unearned insights valuable to Google's competitors. Monsees Decl. ¶ 19.

This group of exhibits contains the kind of internal strategic planning, product development deliberations, performance assessments, and proprietary research that lies at the heart of Google's competitive standing. Information contained within Product Requirements Document (Ex. 4), Objectives & Key Results (Ex. 9), leadership meeting notes (Ex. 19), performance reviews detailing project work (Ex. 10), and internal research compilations (Ex. 33) provide direct insight into Google's priorities, roadmap, internal assessments, and operational strategies. Monsees Decl. ¶¶ 7, 9, 10, 13, 19. Technical details intertwined with strategy discussion (Ex. 2) also reveal Google's proprietary approaches. Monsees Decl. ¶¶ 6. Disclosing this information would allow competitors to anticipate Google's moves, counter its strategies, replicate features without investing in similar research & development, and gain other unfair advantages. *See Psystar*, 658 F.3d at 1162; *Adtrader*, 2020 WL 6391210, at *1.

Google's requests are narrowly tailored. For Exhibits 8, 9, 20, and 29, Google seeks only specific redactions targeting sensitive competitive analyses, OKRs, unrelated internal deliberations, or technical/legal/research details, explicitly *preserving* the portions Plaintiffs actually cite in their Pichai opposition brief. Monsees Decl. ¶¶ 8, 9, 14, 17; *see* Pichai Opp. at 5, 13 (citing Ex. 8), *id* at

5 (citing Ex. 9), *id* at 6, 8, 13 (citing Ex. 20), *id* at 6 (citing Ex. 29). For these, the redactions protect sensitive data without obscuring the factual basis for Plaintiffs' arguments as presented.

For exhibits sought to be sealed entirely (Ex. 2, 4, 10, 19, 33), the sensitive strategic, technical, personnel, and research information is pervasive and inextricably intertwined, making redaction infeasible. Monsees Decl. ¶¶ 6, 7, 10, 13, 19, 24. Moreover, Plaintiffs' reliance on these documents is often minimal or tangential compared to the volume of sensitive content. For example, Exhibit 2 (internal meeting notes) is cited only for a background point about Mr. Pichai's involvement with *some* settings, not the detailed strategic and technical discussions within. Monsees Decl. ¶ 6. Exhibit 4 (PRD) is cited merely for the historical fact that WAA predecessors included "Search History." Monsees Decl. ¶ 7. Exhibit 10 (perf packet) is cited alongside deposition testimony (that Google does not seek to redact) simply to state Mr. Pichai allegedly "sponsored" Firebase. Monsees Decl. ¶ 10. Exhibit 19 (Geo leadership notes) receives only a "*see also*" cite for a proposition regarding Google's response to the 2018 Associated Press story regarding its "Location History Setting." Plaintiffs do not rely on it for any of the months of sensitive Geo strategy discussion contained within. Monsees Decl. ¶ 13. Exhibit 33 (internal research discussions) is cited in a string cite for the high-level point that Mr. Pichai directed teams to make privacy settings simpler, not for the document's underlying cross-product employee feedback. Monsees Decl. ¶ 19. For these exhibits, sealing the entire document is the narrowest way to protect the pervasive confidential information, and doing so would neither obscure the underlying dispute from the public nor curtail Plaintiffs' ability to argue their case publicly.

3. Non-public documents detailing the technical operation of Google's internal systems

Finally, compelling reasons exist to seal confidential technical information concerning the internal operation of systems, as disclosure can harm competitive standing (by revealing proprietary methods) and create security risks (by providing roadmaps for malicious actors). *See Finjan*, 2016 WL 7911651, at *2 (sealing technical information in expert reports and internal documents); *Adtrader, Inc.*, 2020 WL 6391210, at *2 (sealing information revealing capabilities of Google's

systems); *Gmail Litig.*, 2013 WL 5366963, at *3 (same).Google seeks to seal or redact information from the following exhibits containing such technical details:

- Google seeks to seal **Exhibit 27** in its entirety. It presents a highly technical internal assessment concerning a proposal related to retaining WAA-On data. It pervasively contains sensitive technical details (internal servers, specific data logging processes, internal logging "TTLs," data schemas), strategic information (non-public metrics like DAUs, modeling of costs/revenue impacts, fraud/spam detection measures), and internal system links. Monsees Decl. ¶ 15.

- In **Exhibit 28**, an internal Frequently Asked Questions (FAQ) document answering technical questions about WAA data retention changes, Google seeks narrow redactions. These cover a specific non-public user projection (page -531) and proprietary technical details about internal data deletion policies, identification of the specific internal logs affected, links to internal technical documentation, and the methods ensuring downstream systems process deletion signals correctly (page -532). . Monsees Decl. ¶ 16.

- Google seeks to seal **Exhibit 35** in its entirety. This exhibit consists of an internal email thread where engineers discussed a detailed, non-public technical proposal regarding how and where certain location information should be logged within Google's internal systems. It reveals granular specifics about internal data handling processes and maps out aspects of Google's internal data infrastructure, information that is proprietary and potentially exploitable. Monsees Decl. ¶ 21.

- Google seeks to seal **Exhibits 36 and 37** in their entirety. These documents consist of internal notes from recurring one-on-one ("1:1") sync meetings between engineers in Google's Geo organization. Exhibit 36 documents detailed, proprietary technical engineering discussions intertwined with highly confidential personnel and team management matters (including staffing needs, hiring strategy, performance feedback, and potential reorganizations). Exhibit 37 documents primarily technical discussions between engineers regarding the specific internal systems and infrastructure they were developing or maintaining concerning internal location logging. Monsees Decl. ¶¶ 22, 23.

These exhibits contain sensitive technical information about Google's proprietary internal systems, data handling processes, and infrastructure. Disclosure risks significant competitive harm by revealing trade secrets and internal methodologies that competitors could replicate or use to gain an advantage. Monsees Decl. ¶¶ 15, 16, 21, 22, 23. Critically, revealing specifics about data storage, logging mechanisms, deletion processes, server configurations, or internal system architecture could also create security vulnerabilities, providing malicious actors with a roadmap to probe, exploit, or compromise Google's systems or user data. Monsees Decl. ¶¶ 15, 16, 21, 23, 26-27; *see Gmail Litig.*, 2013 WL 5366963, at *3.

Google's redactions in Exhibit 28 are narrowly targeted at the specific technical mechanics of data deletion (policies, logs, downstream effects, URLs) and internal projections, leaving untouched the general statements Plaintiffs cite regarding Mr. Pichai's purported involvement with data retention changes. Monsees Decl. ¶ 16; *see* Pichai Opp. at 8 (citing Ex. 28). For Exhibits 27, 35, 36, and 37, the sensitive technical information (and in Ex. 36, personnel information as well) is so pervasively interwoven that redaction is infeasible. Monsees Decl. ¶¶ 15, 21, 22, 23. Plaintiffs' reliance on these documents is again limited or tangential: Exhibit 27 (technical assessment of WAA retention changes) is cited for the general proposition Mr. Pichai "oversaw and approved data retention policies related to WAA." Pichai Opp. at 13. Plaintiffs do not rely on the deep technical and business information contained throughout. Monsees Decl. ¶ 15. Plaintiffs cite Exhibit 35 (a technical logging email) to mention Mr. Pichai's purported involvement in location coarsening for users with Location History off (in any event, an irrelevant point). They do not, however, cite this document for its discussions throughout Google's proprietary technical architecture and internal logging infrastructure. Monsees Decl. ¶ 21. Plaintiffs cite Exhibits 36 and 37 (engineering 1:1s) generally—and without quoting—for the publicly known fact that Google adopted location coarsening for users with Location History off. They do not, however, rely on these exhibits for their detailed discussion of Geo engineering updates or the confidential personnel matters interwoven with technical details. Monsees Decl. ¶¶ 22, 23. Sealing these documents entirely is necessary to protect the pervasive, sensitive technical and/or personnel details from competitive or malicious exploitation.

The technical information Google seeks to seal, if disclosed, could be exploited by competitors to gain unfair market advantages and by malicious actors seeking to compromise Google's systems or user data. *See Kumandan v. Google LLC*, 2023 WL 2189498, at *2 (N.D. Cal. Feb. 22, 2023) (sealing proprietary information about Google Assistant operations). The nature of this information—including technical documents detailing data flows, server interactions, and internal methodologies—could serve as a roadmap for bad actors attempting to identify vulnerabilities or bypass security measures. *See Adtrader, Inc.*, 2020 WL 6391210, at *2 (sealing information revealing capabilities of Google's systems).

B. References to Internal Code Names and Links

Google seeks narrowly tailored redactions of internal project codenames, internal URLs (pointing to non-public resources like documents, tools, code repositories), and internal technical identifiers (for servers, databases, logs, schemas) where they appear in Plaintiffs Daubert Ex. 6; Google's Pichai Reply; Google's Pichai Reply Appendix A; Exhibits 1, 3, 8, 12, 28, 29, 30, and 31.

Courts routinely recognize compelling reasons to seal these internal names, which are not publicly known and whose disclosure can reveal confidential operational details and create security risks. *See, e.g.*, *Apple, Inc. v. Samsung Elecs. Co.*, 2012 WL 4120541, at *2 (N.D. Cal. Sept. 18, 2012) (sealing "internal code names"); *Bohannon v. Facebook, Inc.*, 2019 WL 188671, at *7 (N.D. Cal. Jan. 14, 2019) (sealing internal task names and URLs); *Gmail Litig.*, 2013 WL 5366963, at *3. Public disclosure risks competitive harm by potentially revealing the focus, nature, or technical underpinnings of non-public projects or systems. Monsees Decl. ¶¶ 26-27. More significantly, it presents security risks: malicious actors could use codenames or technical identifiers to target specific systems or data, and knowledge of internal naming conventions or structures revealed by URLs can aid efforts to probe infrastructure or conduct social engineering attacks. *Id.* Google's request is narrowly tailored, typically redacting most letters of a codename or the entirety of internal URLs and specific technical names, obscuring the identifier while preserving context. Monsees Decl. ¶¶ 5, 28. This Court has previously permitted such redactions. *See, e.g.*, Order Re: Plaintiffs' Administrative Motion to Seal (Dkt. 272) (Dkt. 284); Order Granting in Part and Denying in Part Motion to Seal (Dkt. 353).

C. Non-Public Employee Email Usernames

Finally, Google seeks narrowly tailored redactions of only the unique username portion of non-party Google employees' internal email addresses contained in Google's *Daubert* Opposition Exhibit B, and Pichai Opposition Exhibits 1, 3, 8, 9, 11, 12, 13, 15, 16, 17, 18, 20, 22, 26, 28, 29, 30, 31, 32, 34, 39, and 44. Google proposes redacting only the personal identifier before the "@google.com" domain (*e.g.*, redacting only [uniqueaddress] in First Name Last Name <[uniqueaddress]@google.com>), leaving the employee's name and domain visible. *Id.*

Compelling reasons exist to protect the privacy of current and former Google employees, many of whom are non-parties, from potential harassment, phishing, spam, or other unwanted contact resulting from the public disclosure of their non-public internal email addresses. Monsees Decl. ¶ 25; *See E. & J. Gallo Winery*, 2018 WL 4961606 at *2 (protecting employee privacy); *Music Grp. Macao Com. Offshore Ltd. v. Foote*, 2015 WL 3993147, at *8, 10 (N.D. Cal. June 30, 2015) (sealing employee names/roles). Google does not publicly publish internal email formats or addresses, and has a compelling interest in safeguarding this information for its employees. Monsees Decl. ¶ 25. This Court has previously recognized these interests and ordered such narrowly tailored redactions. *See, e.g.*, Dkt. 284; Dkt. 353. Sealing only the unique username is the narrowest possible means to protect these privacy interests.

IV. CONCLUSION

For the reasons set forth above and in the accompanying Monsees Declaration, Google respectfully requests that the Court grant its narrowly tailored requests and seal the limited information identified herein and in the accompanying [Proposed] Order.

Dated: May 1, 2025

Respectfully submitted,

WILLKIE FARR & GALLAGHER LLP

By: */s/ Benedict Y. Hur*

Benedict Y. Hur
Simona Agnolucci
Eduardo E. Santacana
Argemira Flórez
Harris Mateen

Attorneys for Defendant
GOOGLE LLC